UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	No. 12-cr-847 (PGG)
GILBERTO VALLE,	:	
Defendant.	:	

DEFENDANT GILBERTO VALLE'S MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION FOR A JUDGMENT OF ACQUITTAL ON COUNT TWO

David Patton
Federal Defenders of New York, Inc.
52 Duane Street, 10th Floor
New York, New York 10007
Attorney for Defendant Gilberto Valle

Of Counsel:
Julia Gatto
Robert Baum
Edward S. Zas
John J. Hughes, III
James A. Cohen

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	No. 12-cr-847 (PGG)
GILBERTO VALLE,	:	
Defendant.	:	

PRELIMINARY STATEMENT

Count two of the indictment alleged that Mr. Valle "accessed a computer without authorization and exceeded authorized access" by running a search on May 31, 2012, using a New York City Police Department computer. There is no dispute that on the date in question, Mr. Valle was an officer in the New York City Police Department. There is also no dispute that, as a police officer, Mr. Valle had a valid "Tax ID" and a password that permitted him to access the Department's computers and to run searches—including searches in the federal National Crime Information Center database that he accessed on May 31. If Mr. Valle had a valid law enforcement reason for running the search at issue (for example, if there had been probable cause to believe that the subject of the search was committing a crime), the government's own witness conceded that he would have had the authority to run the search and to obtain the information that he in fact obtained.

In light of these undisputed facts, the only basis for imposing criminal liability in this case is that Mr. Valle's search was not related to his official duties and therefore violated Police Department policies limiting computer use to "official duties and responsibilities." But as numerous courts in this District have held in rejecting similar theories, the plain text of the

Computer Fraud and Abuse Act makes clear that a defendant violates this statute only when he accesses information that the defendant is not entitled to access for *any* purpose—not when the defendant accesses information for personal purposes, in violation of employer policies or regulations limiting computer use to official purposes or official business.

While there is limited authority to the contrary, particularly outside of the Second Circuit, Judge Carter, Judge Cote, Judge Engelmayer, Judge Holwell, Judge Kaplan, and Judge McMahon have all recognized in detailed and thoughtful opinions that these out-of-circuit cases are misguided and unpersuasive. A careful analysis of the plain text and legislative history of the statute shows that it only reaches defendants who obtain information, generally by hacking or stealing passwords, that they have no right to access for any purpose.

That this is so is made clear by Congress's historical amendments to this statute. Prior to 1986, this statute did impose criminal penalties on anyone who misused authorization to a computer system by using the authorization for "*purposes* to which such authorization does not extend." But Congress removed this language in 1986, and explained in the accompanying committee reports that government employees who use their computer access for improper purposes should be subject to administrative sanctions, not criminal punishment. Congress wanted to limit the statute's reach to hacking and similar activities.

Moreover, as the *en banc* Ninth Circuit has explained, any broader theory of liability under the statute as written would lead to absurd results. This statute applies not just to federal databases but to every computer "that affects interstate or foreign commerce," a category that includes essentially every computer connected to the Internet. Employer and government policies restricting computer access to an employee's "official duties and responsibilities" are quite common. Imposing federal criminal liability for every violation of such policies would

ensnare not just employees who look up information that they are not supposed to look up—but also secretaries who play FarmVille on their lunch break and distracted cubicle dwellers who trawl CNN.com in the afternoon.

Congress did not intend to create such expansive federal criminal liability. This Court should join the other judges in this District who have rejected the government's attempts to rewrite this statute, and enter a judgment of acquittal on count two.

STATEMENT OF FACTS

The government alleged that, by querying a New York City Police Department ("NYPD") computer for Maureen Hartigan on May 31, 2012, Mr. Valle violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(B). The indictment charged as follows:

> On or about May 31, 2012 . . . the defendant, intentionally and knowingly accessed a computer without authorization and exceeded authorized access and thereby obtained information from a department and agency of the United States, to wit, VALLE accessed, and obtained information from, the federal National Crime Information Center database, without authorization, and outside the scope of his authority. (Title 18, United States Code, Sections 1030(a)(2)(B).)

(Indictment ¶ 4.)

Mr. Valle had a valid log-in and password to use the NYPD computers, specifically Tax ID 942642. (Tr. 970:7-18, 995:1-13.) A user logged in under Mr. Valle's Tax ID ran a query for "Maureen Hartigan" on May 31, 2012 at 3:43 p.m. (GX 616C; Tr. 582:22-583:8.) The computer system sent the query to a number of law enforcement databases that contain information about individuals with criminal records, including the National Crime Information Center, a New York State parole database, a wanted persons list, and similar law enforcement-related records. (Tr. 583:25-584:2; GX 616E.) Ms. Hartigan had a record only in the driver's license database, which contained her address and a few pieces of basic information from her driver's license. (GX 616E.)

Police officers are trained that they can run queries in the computer system only "within the performance of their duties." (Tr. 914:15-16, 941:2-5; GX 612, at 3.) Officers are "instructed that any accessing of the system f[or] non-work related purposes is improper and illegal." (Tr. 950:1-3.) These rules mean that officers can access the system for some purposes, but not for others. For example, an officer can run a search if he has probable cause to believe a person is committing a crime, or in connection with a traffic stop. (Tr. 974:21-975:8, 977:16-19.) But officers cannot run a search for the purpose of answering a citizen inquiry. (Tr. 975:13-22, 979:16-19, 980:11-16.) The NYPD's official policy on computer use is apparently set forth in the patrol guide, but the patrol guide was not introduced into evidence. (Tr. 983:15:984-6.)

At the close of the government's case, the defense moved for a judgment of acquittal on count two, arguing that "Mr. Valle was an authorized user of a system and the statute was really essentially to cover people who are hackers who hack into a system." (Tr. 1311:22-24.) Counsel for the United States argued in reply that there is "absolutely no legal basis for this argument whatsoever." (Tr. 1319:11-12.)

ARGUMENT

I. THE PLAIN TEXT OF THE CFAA DOES NOT IMPOSE CRIMINAL LIABILITY FOR ACCESSING A COMPUTER FOR AN IMPROPER PURPOSE.

"We must begin, of course, with the plain language of the statute . . . ." *United States v. Robinson*, 702 F.3d 22, 31 (2d Cir. 2012). The CFAA, 18 U.S.C. § 1030(a)(2)(B), provides: "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any department or agency of the United States . . . shall be punished as provided in . . . this section."

The twin prohibitions of access without authorization, and exceeding authorized access, are necessary to prohibit two distinct wrongs: An individual "accesses a computer

without authorization" under this statute if the individual hacks into a computer that he or she has no authority to access at all (*e.g.*, a criminal defendant breaks into a proprietary e-mail system for the U.S. Court of Appeals in an effort to obtain correspondence between panel members). By contrast, a user "exceeds authorized access" if he or she accesses, for example, a data storage facility that contains some files that the user is permitted to access—but hacks into other files that the user is not permitted to access (*e.g.*, a law clerk breaks into his co-clerk's e-mail account, which is maintained on the same computer server as the law clerk's own, authorized e-mail account).

The definition of the term "exceeds authorized access" underscores that liability turns on whether the user was authorized to access the particular *information* at issue, not the purposes for which the user did so. Congress explained: "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter *information* in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (emphasis added). The touchstone of this definition is whether the user was "entitled . . . to obtain" the information in question, not the purpose for the access.

The weight of authority in this Circuit, and all of the persuasive and carefully reasoned cases, have interpreted the statute in this fashion. Six separate judges on this Court have carefully considered and rejected the argument that a § 1030 violation can be established by showing that a user accessed information for an improper purpose—and the Ninth Circuit and Fourth Circuit have also adopted this view. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 863-64 (9th Cir. 2012) (Kozinski, J.) (en banc); *JBCHoldings NY, LLC v. Pakter*, No. 12-cv-7555, 2013 WL 1149061 (S.D.N.Y. Mar. 20, 2013) (Engelmayer, J.); *Advanced Aerofoil Technologies, AG v. Todaro*,

No. 11-cv-9505, 2013 WL 410873 (S.D.N.Y. Jan. 30, 2013) (Carter, J.); *Scottrade, Inc. v. BroCo Investments, Inc.*, 774 F. Supp. 2d 573, 583-84 (S.D.N.Y. 2011) (Holwell, J.); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 190-94 (S.D.N.Y. 2010) (Cote, J.); *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 382-85 (S.D.N.Y. 2010) (Holwell, J.); *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385-86 (S.D.N.Y. 2010) (Kaplan, J.); *Major, Lindsey & Africa, LLC v. Mahn*, No. 10-cv-4329 CM, 2010 WL 3959609 (S.D.N.Y. Sept. 7, 2010) (McMahon, J.).

For example, in *Nosal*, the government charged a former employee with aiding and abetting his former coworkers in "exceed[ing their] authorized access" with intent to defraud. *See* 18 U.S.C. § 1030(a)(4); *Nosal*, 676 F.3d at 856. Shortly after leaving an executive search firm, the defendant convinced his former coworkers to help him start a competing business. While his old coworkers were still employed at his old company, they downloaded source lists from a confidential company database and gave the information to the defendant, in violation of the firm's policy prohibiting disclosure of confidential information. *Id.* The district court dismissed the CFAA charges, and the Ninth Circuit affirmed, ruling that the phrase "'exceeds authorized access' . . . refer[s] to data or files on a computer that one is not authorized to access." *Id.* at 857. The court accepted the defendant's argument that "the statute targets only hackers," and squarely held that "the CFAA does not extend to violations of use restrictions." *Id.* at 856, 863. In other words, a user who did not break in to a computer but merely violated an employer's "use restriction[]" is not criminally liable.

Similarly, in *Aleynikov*, the government alleged that on his last day of employment, Sergey Aleynikov, then a computer programmer at Goldman Sachs & Co., copied "hundreds of thousands of lines of source code" from proprietary software that runs Goldman's

high-frequency trading system. *Aleynikov*, 737 F. Supp. 2d at 175. Aleynikov then made efforts to bring the stolen source code to his new employer in Chicago. *Id.* The U.S. Attorney for the Southern District of New York indicted Aleynikov for violating, *inter alia*, § 1030(a)(2), the same charge now brought against Mr. Valle.[1]

The employer policy allegedly violated in that case was materially indistinguishable from the employer policy at issue here. Goldman Sachs had written policies "limit[ing] access to the Trading System's source code only to Goldman employees who have reason to access that source code," in connection with their official duties and responsibilities at Goldman, "such as the programmers working on the Trading System" for the benefit of Goldman Sachs. 737 F. Supp. 2d at 175; *id.* at 191. In addition, Goldman employees, including Aleynikov, were required to execute written confidentiality agreements. *Id.* at 175.

Judge Cote dismissed the charges, explaining the CFAA's restrictions thusly: "Based on the ordinary meaning of 'authorization,' . . . a person who 'accesses a computer without authorization' does so without any permission at all. By contrast, a person who 'exceeds authorized access' has permission to access the computer, but not the particular information on the computer that is at issue." *Id.* at 191-92. As Judge Cote recognized, "What *use* an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place." *Id.* at 192 (emphasis added). Because Aleynikov was authorized to access the source code as a computer programmer for Goldman Sachs, his access was not unauthorized—even though Aleynikov was accessing the code in order to steal it, which was "in violation of a

[1] The only difference is the jurisdictional element. The basis for federal jurisdiction in this case is that Mr. Valle allegedly obtained information "from a[] department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). In *Aleynikov*, the government invoked § 1030(a)(2)(C), which asserts federal jurisdiction over, *inter alia*, computers used by certain financial institutions. *See* 737 F. Supp. 2d at 190; 18 U.S.C. § 1030(e)(2)(A).

confidentiality agreement or policies or other obligations that the [defendant] owe[d] to the information's owner." *Id.* at 191.

Other judges in this District have reached the same conclusion in civil cases, noting, *inter alia*, that "[t]he CFAA is primarily a criminal statute," so ambiguities concerning its scope should be resolved in favor of lenity. *Scottrade*, 774 F. Supp. 2d at 584; *Playmakers Media*, 725 F. Supp. 2d at 384; *Numerex*, 692 F. Supp. 2d at 386 ("[T]he rule of lenity guides the Court's interpretation of the CFAA, which is primarily a criminal statute.").

As these courts recognized, construing "exceeds authorized access" narrowly is necessary to avoid the absurd results that would follow from the broad interpretation that the government has proposed. If an individual "exceeds authorized access" merely by violating a policy of their employer or of the information provider, the scope of criminal liability under § 1030(a)(2) would be "breathtaking." *Pakter*, 2013 WL 1149061, at *7. In addition to federal government computers, § 1030(a)(2) reaches any "computer affected by or involved in interstate commerce—effectively all computers with Internet access." *Nosal*, 676 F.3d at 859. As a result, the inefficient worker who spent hours trawling Facebook and the New York Times while at work, in violation of an employer's policy limiting computer use to business purposes, would fall squarely within § 1030(a)(2) under the government's proposed interpretation. *Nosal*, 676 F.3d at 860. Even casual Internet users who access social networking or search websites from home and violate the websites' terms and conditions in some minor respect would fall within the government's interpretation of § 1030(a)(2). For instance, "numerous dating websites . . . prohibit inaccurate or misleading information." *Nosal*, 676 F.3d at 861. "Under the government's proposed interpretation of the CFAA, . . . describing yourself as 'tall, dark and

handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit." *Id.* at 862.

Although some courts outside the Second Circuit have imposed liability for accessing a computer for a prohibited purpose, none of those decisions are persuasive, and the Court should follow the persuasive and carefully reasoned decisions of the numerous judges in this District who have considered the arguments of these courts and rejected them. Many of the courts that have imposed "purpose-based" liability appear to have overlooked the issue entirely, often because defense counsel did not raise the issue. *See, e.g.*, *United States v. Slaughter*, 248 F. App'x 313, 314 (3d Cir. 2007) (affirming based on an *Anders* brief that did not mention the issue of whether § 1030(a)(2) was applicable). Others have interpreted the statute in a piecemeal way, without carefully analyzing the plain text. *See, e.g.*, *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010). The Fifth Circuit acknowledged in *John* that it was breaking with the Ninth Circuit and other courts in finding "that access may be exceeded [under the statute] if the purposes for which access has been given are exceeded." *Id.* at 272. But the Fifth Circuit did not acknowledge or consider the absurdities that its reading would create; it did not explain how its interpretation was the best reading of the plain text, which focuses on whether "the accesser is . . . entitled . . . to obtain" the "information," 18 U.S.C. § 1030(e)(6), not what purpose he has for obtaining it; and it failed to explain how its reading was consistent with the rule of lenity.[2]

Judge Cote and Judge Kozinski quite properly rejected the Fifth Circuit's cursory analysis as "unpersuasive." *Aleynikov*, 737 F. Supp. 2d at 193; *Nosal*, 676 F.3d at 862. "Put simply, this other line of cases identifies no statutory language that supports interpreting the CFAA to reach mere misuse or misappropriation of information, let alone language strong

[2] *John* also ignored the legislative history. *See infra* Part II.

enough to justify that interpretation where the rule of lenity counsels a narrow reading." *Playmakers Media*, 725 F. Supp. 2d at 384. The courts that have examined the issue carefully have agreed that merely accessing a computer for improper purposes does not amount to a violation under the statute. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-35 (9th Cir. 2009); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342-43 (N.D. Ga. 2007); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 498-99 (D. Md. 2005). This Court should follow these persuasive authorities.

For this reason, even if all of the government's evidence is believed, the government has failed to prove a § 1030(a)(2)(B) violation. On May 31, 2012, Mr. Valle concededly had authorization to access information in the National Crime Information Center ("NCIC") database—including information about Ms. Hartigan, if he was pursuing a law enforcement purpose. The government's evidence, at best, establishes that Mr. Valle accessed a database that he was permitted to access for some purposes—but did so for a subjective *purpose* that was not permitted by his employer (the New York City Police Department). This is insufficient under the statute, which requires a judgment of acquittal. *See* Fed. R. Crim. P. 29(a); *United States v. Temple*, 447 F.3d 130, 136 (2d Cir. 2006).

Because the plain text of the statute unambiguously forecloses the government's interpretation, the Court's interpretive inquiry is at an end. *See United States v. Gayle*, 342 F.3d 89, 92 (2d Cir. 2003) ("When the words of a statute are unambiguous, then, this first canon is also the last: 'judicial inquiry is complete.'" (internal quotation marks omitted) (quoting *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 254 (1992))). The Court must enter a judgment of acquittal on court two.

II. THE LEGISLATIVE HISTORY ONLY UNDERSCORES THE APPROPRIATENESS OF THIS RESULT.

To the extent that there is any ambiguity in the text of the statute, that ambiguity of course must be resolved in favor of the defendant under the rule of lenity. *United States v. Hammons*, 438 F. Supp. 2d 125, 131 (E.D.N.Y. 2006) ("[I]f any ambiguity exists, it should be resolved in favor of the defendant . . . ."). As the Supreme Court has made clear, "Because construction of a criminal statute must be guided by the need for fair warning, it is rare that legislative history or statutory policies will support a construction of a statute broader than that clearly warranted by the text." *Ratzlaf v. United States*, 510 U.S. 135, 148 (1994) (internal quotation marks omitted) (quoting *Crandon v. United States,* 494 U.S. 152, 160 (1990)). The Second Circuit has gone further, concluding that relying on legislative history to expand the meaning of a criminal statute is impermissible: "[I]t is not consistent with the rule of lenity to construe a textually ambiguous penal statute against a criminal defendant on the basis of legislative history." *United States v. Pabon-Cruz*, 391 F.3d 86, 102 (2d Cir. 2004) (internal quotation marks omitted) (quoting *United States v. R.L.C.,* 503 U.S. 291, 307 (1992) (Scalia, J., concurring)).

Here, moreover, any consideration of the legislative history would only further support the conclusion that the plain text requires. When Congress first created § 1030(a)(2) in 1984, that section imposed a penalty on any defendant who "knowingly accesses a computer without authorization, or having accessed a computer with authorization, *uses the opportunity such access provides for purposes to which such authorization does not extend*," and thereby obtains information. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98–473, § 2102(a), 98 Stat. 1837, 2190 (codified as amended at 18 U.S.C. § 1030)

(emphasis added).[3] As drafted, this language referred specifically to the "purposes" for which the authorization was granted, and it might support a theory like the one that the government has advanced here.

But Congress repealed this language just two years later, replacing it with a new section imposing a penalty only on any defendant who "*intentionally* accesses a computer without authorization, *or exceeds authorized access*, and thereby obtains information." Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, § 2(a)(1), (c), 100 Stat 1213, 1213 (emphasis added). Congress also defined this new language: "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . . ." *Id.* § 2(g)(4), 100 Stat. at 1215 (codified at 18 U.S.C. § 1030(e)(6)). This definition has persisted to the present day. Corresponding textual changes were made in § 1030(a)(3), which covered abuse of government computers.

The 1986 textual changes eliminated any reference to the "purposes" for which information was accessed. That change to the text indicates that Congress did not intend to criminalize accessing information for an improper purpose. *See Nosal*, 676 F.3d at 858 n.5. The reference to "purposes" that was deleted in 1986 was never reinserted into the statute.[4]

---

[3] Although in 1984, § 1030(a)(2) only covered financial institutions, the quoted language also appeared in § 1030(a)(3), which covered government computers.

[4] Congress amended § 1030(a)(2) to cover federal government computers in 1996. *See* Economic Espionage Act of 1996, Pub. L. No. 104–294, § 201(1)(B)(ii), 110 Stat. 3488, 3492. This change closed a gap in the 1986 statute, which prohibited hacking into a federal government computer *only* if the defendant was "without authorization to access *any* computer of [the] department or agency" at issue. *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, § 2(b)(1), 100 Stat 1213, 1213 (codified as amended at 18 U.S.C. § 1030(a)(3)) (emphasis added). Under this language, a janitor employed by the IRS arguably was free to hack into the national tax return database and download

Congress made clear in the committee report that its reason for amending the statute was precisely to prevent prosecutions like this one. As the congressional committee report explained:

> The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct. . . . It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and *peruses data belonging to the department that he is not supposed to look at*. This is especially true where the department in question lacks a clear method of delineating which individuals are authorized to access certain of its data. *The Committee believes that administrative sanctions are more appropriate than criminal punishment in such a case*. The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers—no matter how slightly—he could be prosecuted under this subsection.

S. Rep. No. 99-432, at 7 (1986) (emphasis added), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485.[5] Thus, Congress wanted to foreclose criminal punishment of public employees who might violate a technical restriction against certain kinds of access or uses, especially those that are ambiguous. This cuts against the notion that accessing or using information for an improper purpose could be charged under § 1030. Because purpose is subjective and the scope of employer policies is often open to some doubt, applying the statute to criminalize violations of employer rules would raise the very concerns about ambiguous policies that Congress was trying to avoid.

Congress's discussion of the issue also indicates that it was focused only on individuals who access information to which they have no entitlement, no matter their purpose. For example, by expressing concern about whether government agencies have "a clear method of

---

> every taxpayer's Social Security number if the janitor had an IRS e-mail account. The 1996 amendments plugged this gap.

[5] This language was referring to § 1030(a)(3), not § 1030(a)(2), but this report elucidates the meaning of corresponding textual changes made to § 1030(a)(2).

delineating which individuals are authorized to access certain of its data," Congress indicated that it was contemplating that the statute's application would turn on whether a particular "individual[] [was] authorized to access certain . . . data"—not on what purpose the individual had in doing so. Likewise, as part of the 1986 amendments, Congress changed the scienter requirement in § 1030(a)(2) from "knowingly" to "intentionally," in order "to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data *belonging to another*." S. Rep. No. 99-432, at 6 (1986) (emphasis added), *reprinted in* 1986 U.S.C.C.A.N. at 2484. This further underscores the statute's sole "focus": stopping hackers who access "files or data" that do not belong to them and that they do not have permission to access.

Finally, Congress made clear that it thought "administrative sanctions are more appropriate than criminal punishment" when a government employee misuses access. Congress explicitly "reject[ed]" proposals to "enact as sweeping a Federal statute as possible," because it was confident in "the interests and abilities of the States to proscribe and punish such offenses." *Id.* at 4, *reprinted in* 1986 U.S.C.C.A.N. at 2482. Here, in fact, Mr. Valle was suspended from the police department after this case was filed (and was terminated upon conviction), and the NYPD plainly does have the ability to impose "administrative sanctions" on officers who access law enforcement databases for improper purposes. That appears to be exactly what Congress intended.

In sum, even in the light most favorable to the government, the evidence shows only that Mr. Valle accessed a database for a purpose forbidden by his employer, not that he was unauthorized to access the database at all. Accordingly, the statute does not cover this conduct, and he must be acquitted.

CONCLUSION

For these reasons, the Court should grant Mr. Valle's motion for an acquittal with respect to count two of the indictment.

Dated: New York, New York
June 17, 2013

Respectfully submitted,

David Patton
Federal Defenders of New York

By: /s/ Julia Gatto
Julia Gatto
52 Duane Street, 10th Floor
New York, New York 10007
Attorney for Defendant Gilberto Valle

Of Counsel:
Julia Gatto
Robert Baum
Edward S. Zas
John J. Hughes, III
James A. Cohen